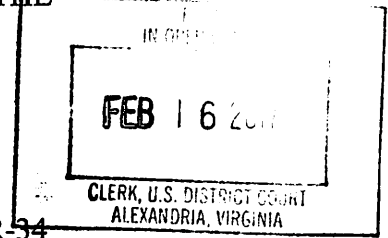


IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

TAYLOR HUDDLESTON,

Defendant.

CRIMINAL NO.: 1:17-CR-34

Count 1: Conspiracy (18 U.S.C. § 371)

Count 2: Aiding and Abetting Computer Intrusions
(18 U.S.C. § 1030(a)(5)(A) and (b), and § 2)

Count 3: Aiding and Abetting Computer Intrusions
(18 U.S.C. § 1030(a)(5)(A) and (b), and § 2)

Forfeiture Notice

Filed Under Seal

FEBRUARY TERM 2017 – AT ALEXANDRIA, VIRGINIA

INDICTMENT

At all times relevant to this Indictment:

1. The defendant, TAYLOR HUDDLESTON, operated a business called “Nimoru Software,” under a particular online alias. Through Nimoru Software, HUDDLESTON developed, marketed, and distributed a licensing software called “Net Seal,” and a remote access trojan called the “NanoCore RAT.”

2. “Licensing software” can be used by legitimate companies to prevent software piracy. Typically, licensing software will generate unique activation codes that purchasers of copyrighted software have to enter in order to activate the copyrighted software. This prevents purchasers of copyrighted software from copying and redistributing the software without the copyright holders’ permission.

3. Net Seal licensing software is licensing software for cybercriminals.

HUDDLESTON understood that developers of illegal computer programs, such as malicious software or “malware,” need licensing software in order to prevent their customers from copying and distributing their malicious software without paying. Accordingly, HUDDLESTON marketed his Net Seal licensing software on an online forum dedicated to computer hacking called Hackforums.net. At all relevant times, HUDDLESTON knew that the purchasers of Net Seal licensing software intended to use it to distribute malicious software that would be used for illegal and unauthorized computer intrusions and, at all relevant times, HUDDLESTON acted with the purpose of furthering and aiding and abetting these illegal and unauthorized computer intrusions and causing them to occur.

4. In addition, HUDDLESTON developed and distributed computer intrusion software known as the NanoCore Remote Access Trojan (“NanoCore RAT”). A remote access trojan, or “RAT,” is a program designed to allow a computer hacker to take complete control of a victim’s computer for the purpose of performing various malicious activities. RATs provide hackers with a backdoor into the infected system of a victim computer so that the hacker can spy on the victim’s computer, cause it to run additional malicious software, or launch attacks on other computer systems. The Nanocore RAT is a widely available and very commonly used remote access trojan that is highly discussed in underground online communities.

5. HUDDLESTON developed and distributed the NanoCore RAT knowing that his customers intended to use it for unauthorized and illegal computer intrusions and, at all times, acted with the purpose of furthering and aiding and abetting these unauthorized and illegal computer intrusions and causing them to occur.

COUNT ONE

(Conspiracy to Aid and Abet Computer Intrusions)

THE GRAND JURY CHARGES THAT:

6. The factual allegations in Paragraphs 1 through 5 are re-alleged and incorporated as if fully set forth here.

7. From at least on or about May 2012, through at least on or about October 2016, in the Eastern District of Virginia and elsewhere, the defendant, TAYLOR HUDDLESTON, did knowingly combine, conspire, confederate, and agree, with Zachary Shames and other persons known and unknown to the Grand Jury, to aid and abet others who knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to protected computers, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 2.

8. In particular, the goal of the conspiracy was to make a financial profit by aiding and abetting computer intrusions, that is, by selling malicious software that would be used for illegal and unauthorized computers intrusions. At all relevant times, HUDDLESTON and his co-conspirators knew and were aware that their customers intended to use, and in fact did use, their malicious software for illegal and unauthorized computer intrusions, and acted with the purpose of furthering and aiding and abetting these illegal and unauthorized computer intrusions and causing them to occur.

Manner and Means

9. As part of the conspiracy, HUDDLESTON developed licensing software called "Net Seal" in order to provide licensing software to developers of malicious software, and to assist in the distribution of malicious software.

10. As part of the conspiracy, HUDDLESTON marketed Net Seal on Hackforums.net, a forum where members can obtain hacking tools and programs and chat with other members on the forum about computer intrusions.

11. As part of the conspiracy, HUDDLESTON accepted payment for Net Seal via PayPal. Generally, HUDDLESTON required his co-conspirators to pay for 50 licenses at a time, meaning that they would buy the right to use Net Seal to distribute 50 copies of malware. During the course of the conspiracy, HUDDLESTON received over 25,000 payments via PayPal from Net Seal customers.

12. As part of the conspiracy, HUDDLESTON was a member of a group on the messaging service "Skype" with approximately seven other prominent members of Hackforums.net, where they could discuss the topic of computer intrusions and the products they were developing. One of the members of this Skype group was Zachary Shames, who was well-known on Hackforums.net as the developer and distributor of a popular keylogger called "Limitless." Limitless allowed users to steal information from victim computers, including sensitive information such as passwords to online banking and email accounts.

13. As part of the conspiracy, HUDDLESTON provided Shames with access to his Net Seal licensing software in order to assist Shames in the distribution of his Limitless keylogger. In exchange, Shames made at least one thousand payments via PayPal to HUDDLESTON. At all times, HUDDLESTON knew that he was assisting in the distribution of the Limitless keylogger, and that the purchasers of keylogger intended to use it and did use it to commit unauthorized and unlawful computer intrusions.

14. As part of the conspiracy, HUDDLESTON set up his Net Seal licensing software to automatically send emails to purchasers of Shames' Limitless keylogger containing the license

serial code and instructions for how to download and activate the keylogger. The purpose of these emails was to help with the orderly, effective, and profitable distribution of the Limitless keylogger.

15. As part of the conspiracy, HUDDLESTON and Shames distributed the Limitless keylogger to over 3,000 people who used it to access over 16,000 computers without authorization with the goal and frequently with the result of stealing sensitive information from those computers.

16. As part of the conspiracy, HUDDLESTON provided Net Seal to several other co-conspirators to assist in the profitable distribution of the malicious software they developed including prolific malware that has repeatedly been used to conduct unlawful and unauthorized computer intrusions.

Overt Acts

17. It was part of the conspiracy that the following acts in furtherance of and to effect the object of the above-described conspiracy were committed in the Eastern District of Virginia and elsewhere:

a. On or about May 8, 2012, Shames, from a computer located in Great Falls, Virginia, within the Eastern District of Virginia, paid HUDDLESTON \$7.40 via PayPal in exchange for using Net Seal licensing software to assist in the distribution of the Limitless keylogger to individuals who intended use Limitless to commit unlawful computer intrusions.

b. On or about July 9, 2012, HUDDLESTON sent an email to Shames in the Eastern District of Virginia containing the code to activate Net Seal.

c. On or about November 21, 2013, HUDDLESTON caused an activation email to be sent to a customer who had purchased the Limitless keylogger, knowing that that

individual intended to use the Limitless keylogger for the purpose of committing unlawful and unauthorized computer intrusions. The email contained the license serial code and instructions for how to download and activate the keylogger.

d. On or about April 23, 2013, Shames, from a computer located in Great Falls, Virginia, within the Eastern District of Virginia, exchanged emails with a customer of Limitless who complained that “the victim’s keyboard after infected will no longer work properly. Victim will call the pc doctor and the logger will be compromised.” In response, Shames assured him: “Trust me. I made this logger. I coded it. It doesn’t change the way the words are typed.”

e. Shames also had several discussions with customers of Limitless on Hackforums.net in which he instructed them on how the Limitless keylogger could be used to steal email and social media passwords from the victim computers. For instance, on or about September 27, 2013, a customer posted: “Confirm ... Outlook recovery WORKING!,” referring to the Keylogger’s ability to recover the victims’ passwords to Microsoft’s popular email service. Shames responded, “Thanks for testing and posting this. I hope you enjoy the new update!”

f. On or about November 2, 2013, a customer asked Shames via Hackforums.net whether the Keylogger “steal[s] saved passwords of [sic] 2014 outlook.” Shames responded: “Yes it should do that. It has the latest recoveries.”

g. On or about November 4, 2013, a customer asked Shames via Hackforums.net : “still waiting to know if it steals 2014 Outlook.” Shames responded: “We are 100% sure it recovers 2013 passwords. If anyone wants to test 2014, feel free.”

h. On or about November 21, 2013, a customer asked Shames via Hackforums.net whether “this is a worm which grabs the login data, log into a facebook/twitter

account and spreads a text.” Shames replied: “yes, it spreads as many posts as you want, and custom ones too!”

(All in violation of Title 18, United States Code, Section 371)

COUNT TWO

(Aiding and Abetting Computer Intrusions and Attempted Computer Intrusions)

THE GRAND JURY FURTHER CHARGES THAT:

18. The factual allegations in Paragraphs 1 through 17 are re-alleged and incorporated as if fully set forth here.

19. From at least on or about May 2012 through on or about December 2014, the defendant, TAYLOR HUDDLESTON, knowingly and intentionally aided and abetted unlawful computer intrusions and attempted unlawful computer intrusions, in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (b), that is, HUDDLESTON knowingly caused the transmission of a program, information, code, and command, and knowingly aided and abetted others in doing the same and in attempting to do the same, and as a result of such conduct, intentionally caused damage and attempted to cause damage without authorization to a protected computer, and resulting in a loss of \$5,000 or more and in damage affecting ten or more protected computers during a one year period, specifically from September 1, 2013 through August 30, 2014.

20. In particular, as alleged in paragraphs 9 through 17 above, HUDDLESON caused, assisted with, and facilitated, the distribution of the Limitless keylogger to over 3,000 individuals who HUDDLESTON knew intended to use, and were using, this malicious software for illegal and unauthorized computer intrusions and attempted computer intrusions. At all relevant times, HUDDLESTON acted with the purpose of furthering these unauthorized and illegal computer intrusions and attempted computer intrusions and causing them to occur.

21. By distributing the Limitless keylogger to over 3,000 accomplices, HUDDLESTON knowingly and intentionally aided and abetted thousands of unlawful computer intrusions and attempted unlawful computer intrusions. The Limitless keylogger that

HUDDLESTON helped distribute infected over 16,000 victim computers, including victim computers in Alexandria, Virginia and Richmond, Virginia, both within the Eastern District of Virginia. The infection of these victim computers by the Limitless keylogger constituted the intentional transmission of a program, information, code, and command that intentionally caused damage without authorization to the protected computers.

(All in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (b), and Section 2)

COUNT THREE

(Aiding and Abetting Computer Intrusions and Attempted Computer Intrusions)

THE GRAND JURY FURTHER CHARGES THAT:

22. The factual allegations in Paragraphs 1 through 21 are re-alleged and incorporated as if fully set forth here.

23. On or about January 2014 through on or about December 2016, the defendant, TAYLOR HUDDLESTON, knowingly and intentionally aided and abetted unlawful computer intrusions and attempted unlawful computer intrusions, in violation of 18 United States Code, Section 1030(a)(5)(A) and (b), that is, HUDDLESTON knowingly caused the transmission of a program, information, code, and command, and knowingly aided and abetted others in doing the same and attempting to do the same, and as a result of such conduct, intentionally caused damage and attempted to cause damage without authorization to a protected computer, and resulting in a loss of \$5,000 or more and in damage affecting ten or more protected computers during a one year period, specifically from December 1, 2015 through November 30, 2016.

24. Specifically, in or about 2013, HUDDLESTON developed and distributed a malicious remote access trojan known as the NanoCore RAT. HUDDLESTON designed the NanoCore RAT for the purpose of enabling its users to commit unauthorized and illegal intrusions against victim computers. HUDDLESTON intentionally marketed the NanoCore RAT to individuals who he knew intended to use it for these malicious purposes.

25. HUDDLESTON advertised the NanoCore RAT on Hackforums.net, and caused it to be distributed to over 350 people who HUDDLESTON knew intended to use, and were using, this malicious software for illegal and unauthorized computer intrusions and for attempted illegal and unauthorized computer intrusions. At all relevant times, HUDDLESTON acted with the purpose of furthering these unauthorized computer intrusions and causing them to occur.

26. By developing the NanoCore RAT and distributing it to hundreds of people who he knew intended to use it for its designated malicious purpose, HUDDLESTON knowingly and intentionally aided and abetted thousands of unlawful computer intrusions and attempted unlawful computer intrusions, including intrusions and attempted intrusions that occurred within the Eastern District of Virginia.

27. HUDDLESTON'S NanoCore RAT was used in a massive "spear phishing" scheme designed to infect and attempt to infect thousands of victim computers, including computers within the Eastern District of Virginia. A spear phishing scheme is a scheme to trick victims into downloading malicious software onto their computer by sending them communications, typically emails, that purport to be from a friendly source and ask the victim to click on a link or open an attachment that looks benign but in fact contains a request to download malicious software.

28. As part of the spear phishing scheme, HUDDLESTON's accomplice created a so-called "spoofed" email address, meaning an email address that appeared to come from a major oil and gas company ("Company 1") but was, in fact, controlled by HUDDLESTON's accomplice. In or about August 2016, HUDDLESTON's accomplice sent emails from this spoofed email address to thousands of targeted victim computers, including a targeted victim computer located in Norfolk, Virginia, within the Eastern District of Virginia. The spear phishing email stated that the victims owed money to Company 1 and included a PDF file attachment that purported to be an invoice from Company 1. The attachment in fact contained a link to a malicious executable that, if clicked by the victim, would send a request to download the NanoCore RAT onto the victim's computer from a remote server. The sending by HUDDLESTON's accomplice of each spear phishing email constituted an attempt to transmit a

program, information, code, and command that would intentionally cause damage without authorization to protected computers.

(All in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (b), and Section 2)

NOTICE OF FORFEITURE

1. There is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

2. The defendant is hereby notified, pursuant to Fed.R.Crim.P. 32.2(a), that upon conviction of an offense set forth in Counts 1-3 of this Indictment, the defendant, TAYLOR HUDDLESTON, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(A), any property constituting, or derived from, proceeds traceable to such violation, and, pursuant to Title 18, United States Code, Section 1030(i)(1), any personal property used or intended to be used to commit or facilitate the offense and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

3. If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Section 982(a)(2)(A) and (B) and 1030(i)(1), as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States of America, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and Title 28, United States Code, Section 2461(c), to seek forfeiture of all other property of the defendant as described in paragraph 2 above.


(All pursuant to Title 18, United States Code, Sections 982(a)(2)(B), and Section 1030(i)(1)).

A TRUE BILL:

Pursuant to the U.S. Government Act,
the original of this page has been filed
under seal in the Clerk's Office.

Foreperson of the Grand Jury

DANA J. BOENTE
UNITED STATES ATTORNEY



Kellen S. Dwyer
Assistant United States Attorney

Ryan K. Dickey
Senior Counsel, Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division